

AMENDMENTS TO THE CLAIMS

Cancel claims 1-18 without prejudice.

Listing of claims:

1-18. (Cancelled)

19. (Previously Presented) A method to enforce privacy preferences on exchanges of personal data of a data-subject, comprising the steps of:

specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints on one or more data-subject data;

receiving a request message from a requester, the request message having one or more requests for one or more of the data-subject data pertaining to the a subject, and a requester privacy statement for each of the respective data-subject data requested, wherein the requester privacy statement includes purpose, retention, recipient, and access information, wherein the purpose information specifies the purpose for which the requested data is acquired, the retention information specifies a retention policy for the requested data, the recipient information specifies the recipients of the requested data, and the access information specifies whether the requested data should be accessible to the data-subject after the data has been released;

comparing the requester privacy statement to the subject constraints; and

releasing the data-subject data in a response message to the requester only if the subject constraints are satisfied.

20. (Previously Presented) The method of claim 19, further comprising the step of

authorizing the requester to receive the data-subject data.

21. (Original) The method of claim 20, wherein the step of authorizing the requester includes the steps of authorization at more than one level.

22. (Previously Presented) The method of claim 19, wherein the step of specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:

specifying an authorization dataset describing the data to which the constraint applies;
specifying a privacy preference rule that describes the privacy preferences under which the data-

subject data may be released and the corresponding actions allowed;

specifying an access list describing who is allowed to access the said data; and

specifying an authorization action that describes any additional action to be taken if the restrictions imposed by the authorization dataset, the privacy preference rule and the access list of this constraint are matched.

23. (Previously Presented) The method of claim 19, wherein the step of specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:

specifying such constraints for subject data that owned and held by the subject;

specifying such constraints for data-subject data that is owned by the data subject, but held by one or more parties on behalf of the subject; and

specifying such constraints for data-subject data that is owned and held by one or more third parties.

24. (Previously Presented) The method of claim 19, wherein the step of specifying one or more data-subject authorization rule sets includes the steps of specifying different data-subject authorization rule sets for the same data-subject data for one or more requesters that must be satisfied for the data-subject data to be released.

25. (Previously Presented) The method of claim 19, wherein the step of comparing the requester privacy statement to the subject constraints includes the step of partitioning the data-subject data into a first part that satisfies the constraints and is released and a second part that does not satisfy the constraints and is not released.

26. (Previously Presented) The method of claim 19, wherein the step of releasing the data-subject data includes the step of getting manual authorization from the data-subject for some of the data-subject data before releasing the data.

27. (Previously Presented) The method of claim 19, wherein the step of releasing the data-subject data includes the step of getting one or more missing values from the data-subject before releasing the data.

28. (Previously Presented) The method of claim 19, wherein the step of releasing the data-subject

data includes the step of getting one or more data-subject data from one or more third parties, that store that data-subject data, before releasing the data.

29. (Previously Presented) The method of claim 19, wherein the step of releasing the data includes the step of providing authorization to one or more third parties holding part of the data-subject data to release the part to the requester.

30. (Previously Presented) The method of claim 19, wherein the step of specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of:

- ordering the data-subject data in a hierarchy with one or more levels; and
- specifying one or more constraints for each level that apply to the data-subject data in that level.

31. (Previously Presented) The method of claim 19, wherein the step of specifying each subject constraint includes the step of specifying one or more of the following: one or more classes of data, one or more properties of data, and one or more instances of data.

32. (Original) The method of claim 30, wherein the step of specifying constraints for each level includes the step of specifying different constraints for one or more of the levels.

33. (Original) The method of claim 30, wherein the step of specifying constraints for each level includes the step of inheriting the constraints from one or more other levels.

34. (Previously Presented) The method of claim 30, wherein the step of ordering the data-subject data into a hierarchy of levels includes the step of creating levels from one or more classes of data, properties of data, instances of data, or a combination thereof these.

35. (Previously Presented) The method of claim 19, wherein the step of specifying one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of specifying constraints that include privacy preferences based on any one or more of a Platform for Privacy Preferences (P3P) standard privacy statements.

36. (Original) A method, as in claim 35 where the standard privacy statements include any one or more of the following: a purpose, a retention, a recipient and an access.

37. (Previously Presented) The method of claim 19, wherein the step of specifying

- one or more data-subject authorization rule sets, the data-subject authorization rule set having one or more subject constraints includes the steps of specifying constraints over subject data that includes any one or more of the following: a privacy data, a privacy data associated a natural person, a confidential information, and a trade secret.